



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/415,461	10/14/1999	RYUICHI AOKI	104526	4858

25944 7590 10/06/2003

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER

CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/415,461

Applicant(s)

AOKI, RYUICHI

Examiner

Paul E. Callahan

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 October 1999.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on ____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). ____. |
| 2) <input checked="" type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>3</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-13 are pending in this application and have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 5-11 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The language of claim 5 is directed towards a client-server model. A review of fig. 1, item 100 indicates that the server and clients are the only discrete entities in the system with the depositories resident on the server as indicated by fig. 1 items 102. The language of claim 5 however, indicates that the depositories are separate entities from the server and are in communication with it via public key encryption. It is unclear from the language of claim 5, when read in light of fig. 1, whether the applicant contemplates the depositories as discrete entities or as resident storage areas or modules on the server that communicate with another recovery module on the server via public key encryption. Claims 6-11 are dependent on claim 5 and are rejected on the same basis as that claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-4, 12, and 13 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Fischer (US 5,436,972).

As per claims 1 and 12, Fischer teaches an encryption key depositing apparatus (Abstract) comprising: a unit that generates an encryption key for a user (col. 1 lines 20-30); and a unit that starts a process in response to the generation of said encryption key (col. 5 lines 24-30, col. 6 lines 25-45), said process allowing a depositary deposited with said generated encryption key to store said key in a subsequently recoverable manner (col. 6 lines 25-45).

As per claim 2, Fischer does not explicitly teach the encryption key depositing apparatus according to claim 1, wherein said encryption key is a private key of a public key cryptosystem, however Fischer does contemplate the user having a public / private key pair (claim 6), and contemplates the escrow of all types of secret data (col. 2 lines 24-36). Therefore it is clear that Fischer does contemplate escrow of a user's private key of a public / private key pair.

Art Unit: 2134

As per claim 3, Fischer teaches the encryption key depositing apparatus according to claim 1, further having rules established as a basis for determining said depositary, said encryption key being stored in accordance with said rules (col. 3 lines 23-30).

As per claim 4, Fischer teaches the encryption key depositing apparatus according to claim 1, further comprising a server and clients (fig. 1), wherein recovery information for recovering said encryption key is encrypted by a public key of said depositary and retained in said server (fig. 5 item 1050, 1060).

As per claim 13, the claim represents a computer program product causing an apparatus to carry out the method of claim 1 and it therefore rejected on the same basis as claim 1.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following documents teach key recovery systems similar to that of the applicant.

Young et al. US 6,282,295

Blaze US 5,721,777

Al-Salqan US 6,549,626

Yahya Al-Salqan: "Cryptographic Key Recovery" IEEE 1997

Pierre-Alain Fouque et al. : "Recovering Keys in Open Networks" IEEE 1999

Art Unit: 2134

Adam Young and Moti Yung: "Auto-Recoverable Auto-Certifiable Cryptosystems" Eurocrypt 1998, LNCS 1403, pp. 17-31.

Dorothy Denning: "Descriptions of Key Escrow Systems" Communications of the ACM 1997.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336.

The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

9/26/03

Paul Callahan